UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

DAVID IRVIN, on behalf of himself and all others similarly situated,

Plaintiff,

v.

CABELA'S L.L.C. and BPS DIRECT, L.L.C.,

Defendants.

Case No. 1:23-cv-00530-CCC

PLANTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

TABLE OF CONTENTS

PAGE(S)

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

In 1995, the Pennsylvania legislature amended the Uniform Firearms Act, adding a provision that requires companies and public entities to keep information about gun ownership confidential. While the legislative history is sparse, the motivations for the amendment are clear. Unlike other consumer goods, knowledge about gun ownership, when given to the wrong person, can have dire, life-threatening consequences. It is no one's business, the Pennsylvania legislature has determined, to know which law-abiding citizens are also gun owners.

In December 2021, David Irvin ("Plaintiff") navigated to cabelas.com, a website operated by Cabela's L.L.C. and BPS Direct L.L.C. ("Defendants"), and he purchased a firearm. While purchasing that firearm, Plaintiff had a reasonable expectation that Defendants would keep the information he entered—like his name, address, and the type of gun he purchased—confidential. Unbeknownst to Plaintiff, Defendants integrated into their website the Facebook Tracking Pixel, a piece of code that, as the name implies, tracked Plaintiff as he browsed for and purchased a firearm, sending to Facebook every button he clicked, page he visited, and form he completed. That conduct, Plaintiff now alleges, violated the Uniform Firearms Act ("UFA") and Pennsylvania's Wiretapping Act ("WESCA").

Defendants have no compelling defense. *First*, Defendants assert that Plaintiff lacks standing, arguing that he fails to allege a concrete injury. But as

numerous courts have held, Plaintiff has suffered a harm that bears a close relationship to privacy torts that have been historically recognized as providing a basis for suit. *Second*, Defendants offer a grab bag of reasons for why Plaintiff's WESCA claim should be dismissed, contending, for example, that Plaintiff fails to allege the Facebook Tracking Pixel constitutes a "device" and that he fails to allege Defendants assisted Facebook with intercepting the "content" of his communications. Each of these arguments are firmly rebutted by Third Circuit authority and Plaintiff's allegations. Defendants end by challenging Plaintiff's UFA claim, arguing that he fails to properly allege a "disclosure" of the information he furnished while purchasing a firearm. Their arguments, however, contravene the statute's plain text and ignore the decisions from Pennsylvania courts saying the opposite. Defendants' motion to dismiss should therefore be denied.

ARGUMENT

I. PLAINTIFF HAS ARTICLE III STANDING

Defendants argue that "Plaintiff lacks standing to bring all of his claims because he has not alleged an actual injury." *See* ECF No. 39, Motion to Dismiss ("MTD") at 5. That argument is incorrect, however, because Plaintiff alleges injuries that bear a close relationship to harms traditionally recognized as providing a basis for suit.

A. Plaintiff Has Standing to Bring His Claim Under the Uniform Firearms Act

Plaintiff plausibly pleads that Defendants violated the Uniform Firearms Act, thereby injuring him in a way that bears a close relationship to the disclosure of private information and intrusion upon seclusion.

As the Supreme Court has recognized, "disclosure of private information[] and intrusion upon seclusion" constitute "harms traditionally recognized as providing a basis for lawsuits in American courts." *TransUnion*, 141 S.Ct. 2190, 2204 (2021). The Third Circuit is in accord, acknowledging that "certain privacy harms, like the disclosure of private information and intrusion of seclusion, have long given rise to tort claims." *See Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155 (3d Cir. 2022). Because those privacy harms are "well-ensconced in the fabric of American law," intangible harms bearing a close relationship to them "qualify as concrete." *See id.* at 155–159 (internal quotations omitted).

Plaintiff alleges that, "[o]n December 2, 2021," he "purchased a firearm from Defendants," and without his "knowledge, consent, or express written authorization," Defendants "disclosed Plaintiff's name, address, his Facebook ID, [and] the type of gun he purchased, among other items." *See* ECF No. 20, First Amended Complaint ("FAC") ¶¶ 9, 69–70. That conduct harmed Plaintiff, disclosing information he deemed "sensitive," "confidential," and "personally identifiable." *Id.* ¶¶ 9, 39, 48. The Pennsylvania legislature made that harm

cognizable by enacting the Uniform Firearms Act, a statute requiring Defendants to keep "[a]ll information" provided by firearm purchasers, including their "name or identity," "confidential." 18 Pa. C.S. § 6111(i). Accordingly, by nonetheless disclosing "protected information about [Plaintiff's] firearms purchases," Defendants created a concrete and cognizable injury. *See* FAC ¶ 9; *see also Susinno v. Work Out World Inc.*, 862 F.3d 346, 352 (3d Cir. 2017) ("Where a plaintiff's intangible injury has been made legally cognizable through the democratic process, and the injury closely relates to a cause of action traditionally recognized in English and American courts, standing to sue exists.").

In nearly identical contexts, courts from across the country—including the Third Circuit—have reached the same conclusion. Those cases concern the Video Privacy Protection Act and Michigan's Preservation of Personal Privacy Act, two statutes that prohibit companies from disclosing information that identifies customers and what they have watched or read. *See* 18 U.S.C. § 2710(b)(1); Mich. Compl. Laws § 445.1712. Under both statutes, both before and after *TransUnion*, courts have uniformly held that unlawful disclosures constitute concrete injuries sufficient to confer Article III standing. *See*, *e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 274 (3d Cir. 2016) ("While perhaps 'intangible,' the harm is also concrete in the sense that it involves a clear *de facto* injury, *i.e.*, the unlawful disclosure of legally protected information."); *Batts v. Gannett Co.*,

2023 WL 3143695, at *3 (E.D. Mich. Mar. 30, 2023) ("[T]he Supreme Court's recent *TransUnion* case does not alter the settled matter of a PPPA violation satisfying Article III standing requirement for a concrete and particularized injury in fact."); *Salazar v. National Basketball Association*, 2023 WL 5016968, at *5 (S.D.N.Y. Aug. 7, 2023) (collecting cases); *Lin v. Crain Communications, Inc.*, 2020 WL 248445, at *6 (E.D. Mich. Jan. 16, 2020) (collecting cases).

These cases apply with full force here. As with the VPPA and the PPPA, the UFA deems a type of information "confidential" and prohibits its "disclosure." 18 Pa.C.S. § 6111(i). Because Defendants disclosed that information anyway, Plaintiff suffered an intangible harm akin to intrusion upon seclusion and disclosure of private information. *Cf. Feldman v. Star Tribune Media Company LLC*, 2023 WL 2388381, at *5 (D. Minn. Mar. 7, 2023) (noting the "evidently close relationship between Feldman's VPPA claim in this case and the intrusion-upon-seclusion tort as it has been traditionally understood"). Plaintiff thus properly alleges a concrete injury.

B. Plaintiff Has Standing to Bring His Claim Under the Pennsylvania Wiretapping Act

Plaintiff has standing to bring his WESCA claim because his injury bears a close relationship to intrusion upon seclusion.

The prevailing view is that a wiretap, by itself, constitutes a concrete injury because it bears a sufficiently close relationship to intrusion upon seclusion. *See,*

e.g., Restatement (Second) of Torts § 652B, cmt. b (listing examples of intrusion upon seclusion, including "tapping … phone lines" and "opening … private and personal mail"); *Raffin v. Medicredit, Inc.*, 2016 WL 7743504, at *3 (C.D. Cal. Dec. 18, 2016) ("Following *Spokeo*, district courts in the Ninth Circuit consistently have concluded that, to satisfy injury in fact, a plaintiff in a CIPA action need not allege actual harm beyond the invasion of the private right conferred by the statute.").

More recently, some courts have held that a wiretap alone is insufficient, requiring that the communications also contain private or personal information. *See, e.g. Massie v. General Motors LLC*, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2023) ("'Eavesdropping' on communications that do not involve personal information, personally identifiable information, or information over which a party has no reasonable expectation of privacy does not amount to a concrete injury."); *see also Lightoller v. Jetblue Airways Corp.*, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023) (holding that, because "no personal information was intercepted or recorded," the plaintiff "has failed to establish injury in fact").

Under either standard, however, Plaintiff still establishes a concrete injury, alleging Defendants "assist[ed] Facebook with interceptions communications that contain sensitive information." *See, e.g.*, FAC ¶ 38. Those communications contained, for example, "Plaintiff's name, address, Facebook ID, [and] the type of

gun he purchased, among other items." *Id.* ¶ 70. That information was not only "personally identifiable," *see id.* ¶ 29, but also "confidential," *see id.* ¶ 48, because it was shielded from disclosure by the Uniform Firearms Act. At no point, moreover, did Defendants ever receive "consent or written authorization." *Id.* ¶ 9. Taken together, under any standard, those allegations are enough to show concrete injury. *See, e.g., In re: Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3d Cir. 2019) ("History and traditional reinforce that a concrete injury for Article standing purposes occurs when Google, or any other third party, tracks a person's internet browser activity without authorization."); *Massie*, 2022 WL 534468, at *5 ("I agree that Plaintiffs have a legally cognizable interest in controlling their personal information and that intrusion upon that interest would amount to a concrete injury.").

Defendants attempts to counter this authority, arguing that, for both claims, Plaintiff lacks standing because "an invasion of privacy requires 'publicity'" and he "only alleges that his information was disclosed to a single entity, Facebook." *See* MTD at 7. As an initial matter, despite the Supreme Court's repeated admonition that "standing is not dispensed in gross," *see Town of Chester, N.Y. v. Laroe Estates, Inc.*, 581 U.S. 433, 439 (2017), Defendants analyze the two claims together. *See* MTD at 5–8. Notwithstanding this, Defendants' argument contravenes Third Circuit authority, ignoring that both claims are analogous to

intrusion upon seclusion, a tort that "does not require publication as an element." *See Borse v. Piece Goods Shop, Inc.*, 964 F.2d 611, 621 (3d Cir. 1992); *see also In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d at 268 (finding Article III standing to assert VPPA and wiretap claims against Viacom and Google where the plaintiffs alleged that those two parties, and only those two parties, "unlawfully used cookies to track children's web browsing and video-watching habits on Viacom's websites"). Defendants' argument can therefore be rejected with ease. [1]

II. PLAINTIFF ADEQUATELY ALLEGES A VIOLATION OF WESCA

A. Plaintiff Alleges an Interception in Pennsylvania

Defendants argue that "Plaintiff fails to allege that a WESCA violation occurred in Pennsylvania" because he "does not allege the location where his information was routed to Facebook's servers." MTD at 9. That is incorrect. Plaintiff alleges that Defendants' interception took place when he was "accessing the website and completing [his] purchase," and that during that time he "was located in Pennsylvania." FAC ¶ 6. In addition, Plaintiff specifically alleges that Defendants' interception took place on his Pennsylvania-based computer because the Facebook Tracking Pixel sent code to his computer that compelled his "browser to send nine cookies to Facebook," including the c_user cookie that

[1] Plaintiff withdraws his request for injunctive relief.

included his Facebook ID. *Id.* ¶¶ 27-31. Likewise, Plaintiff alleges that Defendants configured the Facebook Tracking Pixel to enable Automatic Advanced Matching which compelled his browser to disclose various pieces of data to Facebook. *Id.* ¶¶ 34-36.

Popa v. Harriet Carter Gifts, Inc., 52 F.4th 121 (3d Cir. 2022) confirms that these allegations are sufficient to survive a motion to dismiss. There, the Third Circuit held that "the place of interception is the point at which the signals were routed" to the non-party, including the location of the browser that accessed the website at issue and where the code "began telling the browser to communicate with its servers." *Id.* at 131. Here, Plaintiff adequately states a claim under WESCA because he alleges that Defendants sent code to his computer in Pennsylvania that then compelled his browser to send communications to Facebook. FAC ¶¶ 27-31, 34-36. Because Plaintiff alleges that the code ultimately responsible for the interception, and the browser that was compelled to carry out the interception, were both on his Pennsylvania-based computer, he sufficiently alleges an interception in Pennsylvania. And, as *Popa* points out, ultimately proving those allegations is a fact-intensive exercise that is better determined on summary judgment. *Popa*, 52 F.4th at 131-32 (vacating summary judgment for defendants for, *inter alia*, further factual development regarding the locus of interception).

B. Plaintiff Alleges that the Contents of his Communications were Intercepted

Defendants argue that Plaintiff does not adequately plead a claim under WESCA because he "does not allege what URLs he visited, what buttons he clicked, or any forms he completed on Cabela's website." FAC at 11. That is incorrect. Plaintiff provides ample detail about the contents of his communications on cabelas.com that were intercepted.

WESCA defines "contents" to include "any information concerning the substance, purport, or meaning of that communication." 18 Pa. Cons. Stat. § 5702. Here, Plaintiff adequately alleges that the contents of his communications with cabelas.com were intercepted because he specifies what information Defendants sent to Facebook. *See, e.g.*, FAC ¶ 2 ("Plaintiff Irvin purchased a Henry Big Boy Classic Centerfire Lever-Action Rifle - .45 Colt from cabelas.com"); *id.* ¶ 9 (Defendants "assisted Facebook with intercepting Plaintiff's communications, including those that contained personally identifiable information and protected information about their firearms purchases."); *id.* ¶ 18 (the Facebook Tracking Pixel on Defendants' websites was configured to send "PageView" information to Facebook, which includes the URL accessed); *id.* ¶ 21 (the Facebook Tracking Pixel on Defendants' websites was configured to send "Microdata" information to Facebook, which includes "the title and description of the webpage" visited); *id.* ¶¶ 22-23 (the Facebook Tracking Pixel on Defendants' websites was configured for

"Button Click Automatically Detected" so that clicks on buttons such as "ORDER ONLINE," "ADD TO CART," "CHECKOUT," "CONTINUE," "REVIEW ORDER," and "PLACE ORDER" would be sent to Facebook); *id.* ¶ 24-25 (the Facebook Tracking Pixel on Defendants' websites was configured so that text entered into fields (such as name and address) would be sent to Facebook).

"This event data, jointly and independently, permit an ordinary person to identify what a consumer has viewed and/or purchased on Defendants' websites." *Id.* ¶ 26. Indeed, if one was designing technology to track "information concerning the substance, purport, or meaning" of a user's activity on Defendants' websites, it hard to imagine what else they could even conceivably include. Accordingly, Plaintiff has sufficiently alleged that interception of the contents of his communications. *In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218, at *11 (N.D. Cal. Dec. 22, 2022) ("[B]ecause the 'Log in' button and full-string URLs concern the 'substantive, purport, or meaning of a communication,' these transmissions likely constitute 'contents.'"). And, at worst, Plaintiff sufficiently alleges facts that should be determined at summary judgment rather than on a motion to dismiss. *Popa*, 426 F. Supp. 3d at 119 (stating that "the Court is not disposed to rule on whether any of it constituted 'content' under WESCA as a matter of law at this juncture," and explaining that "[t]he Court will be better equipped to do so after a record is developed").

C. Plaintiff Sufficiently Alleges that His Communications were Intercepted Through the Use of a Device or Apparatus

Defendants argue that Plaintiff does not allege the use of a device for purposes of WESCA because "a device does not encompass intangible software code on a website." MTD at 14-15. That is incorrect. WESCA defines "intercept" to include "any electronic, mechanical or other device," which it in turns defines to include "**[a]ny** device or apparatus" that can be used to intercept electronic communications. 18 PA. C.S.A. § 5702 (emphasis added). "The use of the word 'any' before the phrase 'device or apparatus' in Section 5702 implies that the class of technology contemplated by WESCA is broad." *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 117 (W.D. Pa. 2019); *id.* at 166 ("WESCA defines the term 'device' broadly . . . ."). In addition, the Facebook Tracking Pixel does not fall within any of WESCA's exceptions to the definition of "devices" which "must be construed narrowly." *Id.* And, at the end of the day, whether particular computer "code qualifies as a 'device' or 'apparatus' is a fact intensive inquiry that implicates novel questions" and "[t]he discovery process will give the parties an opportunity to develop a record that contextualizes the conduct at issue in light of this statutory language." *Id.*

Defendants do not cite to a single case interpreting WESCA so narrowly that it excludes computer code. To the contrary, the Third Circuit has assumed that software counts as a device under WESCA. *See Popa*, 52 F.4th at 131 n.8; *see also*

Commonwealth v. Smith, 136 A.3d 170, 178 (Pa. Super. Ct. 2016) (an app that can record conversations "constitute[s] an interception 'device' under the Wiretap Act"). And courts interpreting parallel wiretapping statutes have routinely held that computer code counts as a device. *United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) ("The majority of courts to consider this issue have entertained the notion that software may be considered a device for the purposes of the [federal] Wiretap Act."); *Luis v. Zang*, 833 F.3d 619, 630 (6th Cir. 2016) (accepting that a software could be a "device"); *In re Carrier IQ, Inc.*, 78 F.Supp.3d 1051, 1087 (N.D. Cal. 2015) (concluding that a software was an "electronic, mechanical or other device"); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661-62 (E.D. Ten. 2012) (analyzing spyware software as a device); *Shefts v. Petrakis*, 2012 WL 4049484, at *8-9 (C.D. Ill. 2012) (analyzing software as a device); *United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011) (accepting that a keylogger software could be considered a scanning receiver, or a device, under 18 U.S.C. § 1029(e)(8)).

D. Plaintiff Did Not Consent to the Interception of His Communications

Defendants argue that Plaintiff's WESCA claim fails as a matter of law because Facebook and Defendants both purportedly obtained his consent to the interception. That is incorrect. Facebook expressly states that it only intercepts data when third-parties like Defendants have the lawful right to share such data.

Here, because Plaintiff never gave Defendants consent to share his firearm purchase data, their violation of WESCA and the UFA are not excused by Facebook's policies.

Defendants contend that Plaintiff consented to Facebook's Cookie's Policy which states that Facebook tracks users' "off-Facebook activity." MTD at 17. As an initial matter, "a district court may not consider matters outside of the Complaint when ruling on a motion to dismiss." *Cerome v. Moshannon Valley Corr. Ctr./Cornell Companies, Inc.*, 2010 WL 4948940, at *3 (3d Cir. Dec. 7, 2010). In addition, Defendants have not made any showing that Plaintiff ever agreed to Facebook's Cookies Policy, let alone the version that it attaches to its motion.

Regardless, as one recent case made clear, even if Plaintiff had agreed to that policy, it would not constitute consent to the interception at issue. In *In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218 (N.D. Cal. Dec. 22, 2022), the plaintiffs alleged that Meta used the Facebook Tracking Pixel to obtain their healthcare-related information from various websites. Like Defendants here, Meta argued that the plaintiffs consented to that interception because its policies "notify Facebook users that [it] collects and uses their personal data, including data about their browsing behavior on some third-party websites, at least in part for targeted advertising." *Id.* at *9 (citing Meta's Cookie Policy and Terms of Service). The

court disagreed, holding that Meta's "generalized notice" was not sufficient to establish consent to interception of health data in particular. *Id.* In addition, the court relied on Facebook's separate representation to users that it "requires" any third-party to have "lawful rights to collect, use and share your data before providing any data to us." *Id.* at *10 (quoting Meta's Data Policy).

The same reasoning applies here. Even if Defendants could demonstrate that Plaintiff agreed to Meta's Cookie Policy, the scope of that consent is limited by Meta's Data Policy and therefore turns on whether Defendants were entitled to share that data in the first instance. Here, given the application of WESCA and the UFA to the disclosures at issue, it was not. *See* FAC ¶ 43 (reviewing Facebook's Data Policy and observing it expressly represents that Facebook requires "partners," like Defendants, "to have lawful rights to collect, use, and share your data before providing any data to us"); *see also* ¶ 45 (reviewing public representations from Facebook stating that the social media site "prohibit[s] businesses or organizations from sharing sensitive information with us").

Nor have Defendants demonstrated that they procured consent themselves to avoid violating those statutes. Defendants argue that Plaintiff "consented to BPS's use of the Facebook Pixel by accepting BPS's privacy policy," but it provides zero evidence of such an acceptance. While Defendants state that the policy (which it does not even bother to attach to its motion) was "publicly-posted" on its website,

that kind of a browsewrap agreement does not constitute an enforceable contract because it does not involve any action (such as clicking "I Agree") that would manifest assent. *See James v. Glob. TelLink Corp.*, 852 F.3d 262, 267 (3d Cir. 2017) ("When terms are linked in obscure sections of a webpage that users are unlikely to see, courts have refused to find constructive notice."); *Childs v. Fitness Int'l LLC*, 2023 WL 3594180, at *3 (E.D. Pa. May 22, 2023) ("Standing alone, using a website is not sufficient to form a contract under Pennsylvania law, and is exactly the type of browsewrap agreement courts across the country refuse to enforce."). Accordingly, Defendants have not demonstrated that Plaintiff gave either them or Facebook consent to the disclosures at issue.

III. PLAINTIFF PROPERLY PLEADS THAT DEFENDANTS VIOLATED THE UNIFORM FIREARMS ACT

A. Plaintiff Properly Alleges that Defendants' Transmissions to Facebook Constitute a "Disclosure"

Defendants contend that the UFA claim must fail because Defendants "cannot simultaneously be the party responsible for 'intercepting' a communication and also for 'procuring' Facebook to commit an interception." MTD at 23. That argument has been rejected by every court to consider it.

As explained, by integrating the Facebook Tracking Pixel into their websites, Defendants assisted Facebook with intercepting Plaintiff's communications. *See, e.g., Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at

*2 (N.D. Cal. Oct. 23, 2019) ("Although Moosejaw cannot be liable for eavesdropping on its own communications with Revitch, the complaint adequately alleges that Moosejaw violated section 631 by enabling Navistone's wrongdoing."). At the same time, "[b]y installing the Pixel, Defendant[s] opened a digital door and invited Facebook to enter that door and extract information from within." *Czarnionka v. Epoch Times Association, Inc.*, 2022 WL 17069810, at *3 (S.D.N.Y. Nov. 17, 2022). As courts have uniformly held, that conduct "is sufficient to constitute [a] 'disclosure.'" *See id.*; *see also Harris v. Public Broadcasting Service*, 2023 WL 2583118, at *5 (N.D. Ga. Mar. 20, 2023) (rejecting the argument that the allegations fail to show "any disclosure by PBS of her information to Facebook," observing that "Plaintiff clearly alleges Defendant, through the Facebook pixel, sent Plaintiff's FID and the URLs of the videos she watched to Facebook"); *Belozerov v. Gannett Co.*, 2022 WL 17832185, at *3 (D. Mass. Dec. 20, 2022) (rejecting the defendant's argument that "it did not actually 'disclose' any PII to Facebook," finding sufficient that the plaintiff "alleges throughout the complaint that defendant inserted the code into the USA Today website to transmit users' information to Facebook").

B. Plaintiff Properly Alleges that the Uniform Firearms Act Protects the Information that Defendants Disclosed

Defendants next argue that "the confidentiality provision of the UFA only applies to an 'application/record of sale,' which is simply not at issue here." *See*

MTD at 24. But that argument gets the law wrong, ignoring the statute's plain text.

It is well established that "courts must presume that a legislature says in a statute what it means and means in a statute what it says there," *see Connecticut Nat. Bank v. Germain*, 503 U.S. 249, 253–54 (1992), so if the Pennsylvania legislature intended to limit the UFA's confidentiality provision to only information on the "application/record of sale," then it would have said so explicitly. Instead, the Pennsylvania legislature chose to protect "[a]ll information" that a purchaser "furnishes" when completing a transaction for a firearm. *See* 18 Pa. C.S. § 6111(i). That aligns with rulings from Pennsylvania's Office of Open Records, which has consistently held that the UFA's confidentiality provision broadly protects any information provided while purchasing a firearm. *See Deckant v. Wayne County Sheriff's Office*, 2018 WL 381772, at *3 (Pa. Off. Open. Rec. Aug. 6, 2018) ("This information, whether contained in the underlying application or license, or collected and maintained in the course of transferring a firearms license, is protected by the relatively broad confidentiality provision within the Firearms Act and its implementing regulations."); *see also Sibley v. Lehigh County*, 2022 WL 30988196, *3 (Pa. Off. Open. Rec. Aug. 1, 2022) (same).

Here, Plaintiff alleges that, while purchasing a firearm, he furnished his "name" and "address," along with information identifying "the type of gun he purchased." FAC ¶ 70. Then, "without consent or written authorization," Defendants disclosed this information to Facebook. *See, e.g.*, *id.* ¶ 9. Because this information was "collected and maintained in the course of [purchasing] a firearm," *see Deckant v. Lancaster County Sheriff's Office*, 2018 WL 3739100, at *4 (Pa. Off. Open Rec. Aug. 2, 2018), Defendants violated the UFA by disclosing it.

But even if the UFA only shields information on "applications/records of sale," *see* MTD at 24, Plaintiff's allegations are sufficient. Plaintiff alleges he "purchased a Henry Big Boy Class Centerfire Lever-Action Rifle -.45 Colt from cabelas.com." FAC ¶ 69. When Plaintiff purchased that firearm, Defendants disclosed when he clicked "PLACE ORDER," *id.* ¶ 23, which also disclosed the "content that [he] enter[ed] into form fields," *id.* ¶ 24, like his first name, last name, address, phone number, and email address, *see* ¶ 25. Plaintiff provided that information while completing the transaction—in other words, while completing an application of sale—so even under Defendants' narrow interpretation, his UFA claim still survives.

C. Plaintiff Properly Alleges that the Uniform Firearms Act Protects the Information that Defendants Disclosed

Defendants then asserts that, "[e]ven if there were an improper 'disclosure' here, Plaintiff does not allege a 'public' disclosure as required by the statute's plain text." MTD at 25. But far from being required by the statutory text, Defendants' interpretation would defeat the statute's purpose.

As an initial matter, an appellate court in Pennsylvania has already rejected Defendants' interpretation, reversing a lower court's ruling and concluding that, "given the extent to which the General Assembly built confidentiality into the UFA, we cannot agree with common pleas' construction of the term 'public disclosure' in Section 6111(i) as incorporating the requirement of 'publicity' necessary to prove the common law tort of invasion of privacy." *See Doe v. Franklin County*, 139 A.3d 296, 306 (Pa. Commw. Ct. 2016), *rev'd on other grounds*, 644 Pa. 1 (2017). Instead, "the General Assembly included both the term 'confidential' and the phrase 'not subject to public disclosure' in Section 6111(i) so that issuing sheriffs may disclose the information to those necessary for law enforcement or criminal justice purposes." *Id.* "Disclosure to any other person constitutes 'public disclosure' for purposes of this section." *Id.* at 307; *see also id.* ("Any other interpretation of Section 6111(i) … would be inconsistent with the UFA's purpose and structure.").

Along with conflicting with the view of a Pennsylvania appellate court, Defendants' interpretation would also defeat the statute's purpose. Under Defendants' interpretation, anyone could file a public information request and receive firearms records so long as they are "one entity" and not "numerous individuals." MTD at 25. Because that would create an easy workaround and render the confidentiality provision a nullity, that construction should be defeated. *See Wiesheier v. Kessler*, 311 Pa. 380, 384 (1933) ("Where, on a reasonable interpretation, a statutory provision is susceptible of a construction which will carry into effect the avowed purpose of the act, that construction should be given to it, rather than one which in practical operation might defeat such purpose."). As such, because Plaintiff properly alleges a disclosure to Facebook, Defendants' conduct amounts to a UFA violation.

CONCLUSION

For the foregoing reasons, Defendant's Motion should be denied in full.

Dated: August 11, 2023

Respectfully submitted,

/s/ Joshua D. Arisohn

BURSOR & FISHER, P.A.
Joshua D. Arisohn
Philip L. Fraietta*
1330 Avenue of the
Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150

Fax: (212) 989-9163
jarisohn@bursor.com
pfraietta@bursor.com

BURSOR & FISHER, P.A.
Christopher R. Reilly*
701 Brickell Avenue, Suite 1420
Miami, FL 33131
Tel: (305) 330-5512
Fax: (305) 679-9006
creilly@bursor.com

**Pro Hac Vice Application Forthcoming*

CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
Steven A. Schwartz (PA I.D. No. 50579)
361 W. Lancaster Avenue
Haverford, PA 19041
Tel: (610) 642-8500
Fax: (610) 649-3633
E-Mail: sas@chimicles.com

Attorneys for Plaintiff